P⊘RTAL

USPTO

Search: ⦿ The ACM Digital Library   ○ The Guide

("isolated execution" and attack)

SEARCH

THE ACM DIGITAL LIBRARY

🖵 Feedback

("isolated execution" and attack)
Terms used: **isolated execution   attack**

Found **9** of 2:

Sort results by [relevance ▼]   ❧ Save results to a Binder

Display results [expanded form ▼]   ☐ Open results in a new window

Refine these results with Advance
Search
Try this search in The ACM Guide

Results 1 - 9 of 9

---

1   Energy and execution time analysis of a software-based trusted platform module
Najwa Aaraj, Anand Raghunathan, Srivaths Ravi, Niraj K. Jha
April 2007 **DATE '07:** Proceedings of the conference on Design, automation and test in Europe
Publisher: EDA Consortium
Full text available: 🗎 pdf(838.82 KB) Additional Information: full citation, abstract, references

Trusted platforms have been proposed as a promising approach to enhance the security of general-purpose computing systems. However, for many resource-constrained embedded systems, the size and cost overheads of a separate Trusted Platform Module (TPM) ...

---

2   Externally verifiable code execution
Arvind Seshadri, Mark Luk, Adrian Perrig, Leendert van Doorn, Pradeep Khosla
September 2006 **Communications of the ACM,**   Volume 49 Issue 9
Publisher: ACM

Additional Information: full citation, abstract, references, index terms

Full text available: 🗎 pdf(194.20 KB) 🗎 html(25.88 KB)

Using hardware- and software-based techniques to realize a primitive for externally verifiable code execution.

---

3   Is a bot at the controls?: Detecting input data attacks
Travis Schluessler, Stephen Goglin, Erik Johnson
September 2007 **NetGames '07:** Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games
Publisher: ACM
Full text available: 🗎 pdf(158.00 KB) Additional Information: full citation, abstract, references, index terms

The use of programmatically generated input data in place of human-generated input data poses problems for many computer applications in use today. Mouse clicks and keyboard strokes can automatically be generated to cheat in online

---

games, or to perpetrate ...

Keywords: cheat detection, cheating, online games, security

4 A feather-weight virtual machine for windows applications

Yang Yu, Fanglu Guo, Susanta Nanda, Lap-chung Lam, Tzi-cker Chiueh
June 2006 **VEE '06:** Proceedings of the 2nd international conference on Virtual
execution environments
Publisher: ACM

Full text available: pdf(192.18 KB)   Additional Information: full citation, abstract, references, index terms

Many fault-tolerant and intrusion-tolerant systems require the ability to execute
unsafe programs in a realistic environment without leaving permanent
damages. Virtual machine technology meets this requirement perfectly because
it provides an execution ...

Keywords: copy on write, mobile code security, namespace virtualization,
system call interception, virtual machine

5 Secure virtual architecture: a safe execution environment for commodity operating systems

John Criswell, Andrew Lenharth, Dinakar Dhurjati, Vikram Adve
October 2007 **SOSP '07:** Proceedings of twenty-first ACM SIGOPS symposium on
Operating systems principles
Publisher: ACM

Full text available: pdf(383.30 KB)   Additional Information: full citation, abstract, references, index terms

This paper describes an efficient and robust approach to provide a *safe
execution environment* for an entire operating system, such as Linux, and all its
applications. The approach, which we call *Secure Virtual Architecture* (SVA),
defines ...

Keywords: compiler, memory safety, operating systems, security, type safety,
typed assembly language, virtual machine

6 Implementing middleware for content filtering and information flow control

Jeffrey Choi Robinson, W. Scott Harrison, Nadine Hanebutte, Paul Oman, Jim
Alves-Foss
November 2007 **CSAW '07:** Proceedings of the 2007 ACM workshop on Computer
security architecture
Publisher: ACM

Full text available: pdf(167.37 KB)   Additional Information: full citation, abstract, references, index terms

This paper discusses the design and implementation of a middleware guard for
purposes of content filtering and information flow control in the Multiple
Independent Levels of Security (MILS) architecture. The MILS initiative is a joint
research effort ...

Keywords: CORBA, GIOP, IIOP, MILS, MLS, common criteria, guards, high
assurance, safety, security

7 Container-based operating system virtualization: a scalable, high-performance alternative to hypervisors

Stephen Soltesz, Herbert Pötzl, Marc E. Fiuczynski, Andy Bavier, Larry Peterson
June 2007 **ACM SIGOPS Operating Systems Review**,   Volume 41 Issue 3
Publisher: ACM

Full text available: pdf(863.93 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Hypervisors, popularized by Xen and VMware, are quickly becoming commodity. They are appropriate for many usage scenarios, but there are scenarios that require system virtualization with high degrees of both *isolation* and *efficiency*. Examples ...

Keywords: Linux-VServer, Xen, alternative, container, hypervisor, operating, system, virtualization

8 Container-based operating system virtualization: a scalable, high-performance alternative to hypervisors

Stephen Soltesz, Herbert Pötzl, Marc E. Fiuczynski, Andy Bavier, Larry Peterson
March 2007 **EuroSys '07:** Proceedings of the ACM SIGOPS/EuroSys European Conference on Computer Systems 2007
Publisher: ACM

Full text available: pdf(863.93 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Hypervisors, popularized by Xen and VMware, are quickly becoming commodity. They are appropriate for many usage scenarios, but there are scenarios that require system virtualization with high degrees of both *isolation* and *efficiency*. Examples ...

Keywords: Linux-VServer, Xen, alternative, container, hypervisor, operating, system, virtualization

9 Symmetric behavior-based trust: a new paradigm for internet computing

Vivek Haldar, Michael Franz
September 2004 **NSPW '04:** Proceedings of the 2004 workshop on New security paradigms
Publisher: ACM

Full text available: pdf(76.86 KB) Additional Information: full citation, abstract, references

Current models of Internet Computing are highly asymmetric - a host protects itself from malicious mobile Java programs, but there is no way to get assurances about the behavior of a program running remotely. The asymmetry stems from a behavior-based ...

Results 1 - 9 of 9